Daily Open Source Infrastructure Report
16 April 2015

Top Stories

- Court documents unsealed April 14 revealed that a man charged in the March 13 robbery of a Wells Fargo bank branch in Washington, D.C., confessed to 8 other robberies perpetrated by the "Black Hat Bandits" gang. – *Washington Post* (See item **4**)
- A Government Accountability Office report released April 14 warned that commercial flights with Internet-based technology are vulnerable to having their onboard systems hacked remotely through the plane's Wi-Fi network. – *Associated Press* (See item **5**)
- A North Palm Beach-based ophthalmologist was charged April 14 in connection to a scheme to allegedly defraud Medicare and other healthcare programs out of over $105 million through the submission of fake claims. – *Reuters* (See item **12**)
- Findings from Verizon's recently released annual Data Breach Investigations Report revealed that the top industries affected by data breaches in the last year were public administration, financial services, manufacturing, accommodations, and retail, among other findings. – *IDG News Service* (See item **26**)

Fast Jump Menu

Energy Sector

1. *April 14, Associated Press* – (Ohio) **FirstEnergy to close 3 northeast Ohio coal-burning plants.** FirstEnergy reported April 14 that 3 coal-burning power plants in Ohio will be closed and secured in a safe and environmentally compliant condition April 15 as part of the company's plan to comply with U.S. Environmental Protection Agency regulations on emissions of mercury and other air pollutants.
Source: http://www.whio.com/ap/ap/ohio/firstenergy-to-close-3-northeast-ohio-coal-burning/nks9Q/

For another story, see item **15**

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

2. *April 15, Pottstown Mercury* – (Pennsylvania) **Limerick nuke plant outage starts with a hiccup.** U.S. Nuclear Regulatory Commission officials reported that a failure in a nuclear monitoring instrument drawer caused an unplanned scram in Exelon Nuclear's Limerick Nuclear Generating Station's Unit 2 reactor in Pennsylvania April 13 while the reactor was being shut down for scheduled maintenance and refueling. The malfunctioning drawer was bypassed in a subsequent reset and will be repaired during the outage.
Source: http://www.pottsmerc.com/general-news/20150414/limerick-nuke-plant-outage-starts-with-a-hiccup

[Return to top]

Critical Manufacturing Sector

See item **26**

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

3. *April 15, Softpedia* – (National) **Users in the U.S. targeted with ransomware via tax return-flavored emails.** Security researchers at Kaspersky Lab identified a phishing scheme in which cybercriminals send emails purportedly from the U.S. Internal Revenue Service regarding tax refunds which contain rigged Microsoft Word files that download a trojan once macros are enabled. The trojan blocks access to the Internet and demands payment to a short message service (SMS) number via prepaid cards.
Source: http://news.softpedia.com/news/Users-in-the-US-Targeted-with-Ransomware-Via-Tax-Return-Flavored-Emails-478465.shtml

4. *April 14, Washington Post* – (Washington, D.C.; Maryland; Virginia) **Police link man arrested in D.C. bank robbery to Black Hat Bandits.** Court documents unsealed April 14 revealed that a man charged in the March 13 robbery of a Wells Fargo bank branch in Washington, D.C., confessed to 8 other bank robberies perpetrated by the "Black Hat Bandits" gang throughout Virginia and Maryland since January. Authorities are seeking other suspects linked to the nine robberies.
Source: http://www.washingtonpost.com/local/crime/police-link-man-arrested-in-dc-bank-robbery-to-black-hat-bandits/2015/04/14/9653db5c-e2ab-11e4-81ea-0649268f729e_story.html

For another story, see item **26**

[Return to top]

Transportation Systems Sector

5. *April 15, Associated Press* – (National) **GAO reports warns hackers could bring down plane using passenger Wi-Fi.** A Government Accountability Office report released April 14 warned that commercial flights that have been modernized with Internet-based technology are vulnerable to having their onboard systems hacked remotely through the plane's passenger Wi-Fi network. The report states that airlines are currently relying on firewalls to create a barrier between the avionics in a cockpit and passenger Wi-Fi networks.
Source: http://www.foxnews.com/tech/2015/04/15/gao-reports-warns-hackers-could-bring-down-plane-using-passenger-wi-fi/

6. *April 14, WFTV 9 Orlando* – (Florida) **Jackknifed tractor-trailers cause delays for more than 7 hours on I-95 near Ormond Beach.** A stretch of Interstate 95 Northbound in Volusia County reopened after being closed for more than 7 hours April 13 – 14 while HAZMAT crews cleared the scene where 2 semi-trucks had jackknifed and spilled about 50 gallons of diesel fuel onto the roadway.
Source: http://www.wftv.com/news/news/local/stretch-i-95-nb-shut-down-volusia-due-jackknifed-t/nksw6/

7. *April 14, KSTU 13 Salt Lake City* – (Utah) **I-80 lanes at Utah/Nevada border reopen for travel after multi-car pileup.** All lanes of Interstate 80 reopened April 14 after westbound traffic at mile marker 99 was closed for several hours and eastbound traffic was closed to high profile vehicles, after strong wind gusts resulted in overturned semi-

trucks and a multi-vehicle accident near the Utah/Nevada border that killed 1 person and injured 25 others.
Source: http://fox13now.com/2015/04/14/high-winds-force-lane-closures-on-i-80-at-utahnevada-border/

8. *April 14, WHIO 7 Dayton* – (Ohio) **911 call about wrong way driver came 16 seconds before crash.** Interstate 70 East in Clark County reopened April 14 after being closed for approximately 4 hours when a wrong-way driver fatally crashed into a semi-truck head-on. The cause of the crash remains under investigation.
Source: http://www.whio.com/news/news/crash-seme-fire-closes-interstate-70/nktCp/

[Return to top]

Food and Agriculture Sector

9. *April 14, Associated Press* – (Iowa) **Bird flu confirmed in Iowa turkey flock.** The Iowa Department of Agriculture confirmed April 14 the presence of the H5N2 strain of bird flu virus in a barn on a farm housing 27,000 birds in Buena Vista County. The farm was placed under quarantine and the flock's remaining turkeys will be culled as a precaution.
Source: http://www.kcci.com/news/bird-flu-confirmed-in-iowa-turkey-flock/32363486

10. *April 14, Associated Press* – (Minnesota) **Deadly bird flu confirmed at 8 more Minnesota turkey farms.** Authorities confirmed news cases of the H5N2 bird flu virus at 8 Minnesota turkey farms, and ordered the farms' 542,500 turkeys be culled to prevent the disease from spreading. The affected farms were quarantined as a precaution.
Source: http://minnesota.cbslocal.com/2015/04/14/deadly-bird-flu-confirmed-at-8-more-minnesota-turkey-farms/

11. *April 14, U.S. Department of Agriculture* – (National) **Beech-Nut Nutrition recalls baby food product due to possible foreign matter contamination.** The Food Safety and Inspection Service announced April 14 that Beech-Nut Nutrition issued a recall for about 1,920 pounds of its Stage 2 Beech-Nut Classics Sweet Potato & Chicken product due to possible contamination with small pieces of glass. The recall was issued after the firm received a report of an oral injury
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-061-2015-release

[Return to top]

Water and Wastewater Systems Sector

Nothing to report

[Return to top]

Healthcare and Public Health Sector

12. *April 14, Reuters* – (Florida; New Jersey) **Florida doctor indicted on Medicare fraud: U.S. Attorney.** A North Palm Beach-based ophthalmologist was charged April 14 in connection a scheme to allegedly defraud Medicare and other healthcare programs by billing Medicare for more than $190 million, and receiving over $105 million in reimbursements through the submission of fake claims and false diagnoses. The doctor was also charged with corruption along with a New Jersey senator after they allegedly traded up to $1 million worth of gifts in exchange for political favors.
Source: http://www.reuters.com/article/2015/04/14/us-usa-florida-melgen-idUSKBN0N52JP20150414

13. *April 14, SC Magazine* – (California) **California-based home care services co. notifies employees of data breach, tax fraud.** California-based Homebridge, formally known as In-Home Supportive Services (IHSS) Consortium notified an undisclosed amount of current and former employees that their personal information as well as Social Security numbers may have been accessed after a limited number of computers were infected with malware from January to March. The company is investigating the breach and stated that hackers gained unauthorized access to human resource records.
Source: http://www.scmagazine.com/california-based-home-care-services-co-notifies-employees-of-data-breach-tax-fraud/article/409006/

For another story, see item **15**

[Return to top]

Government Facilities Sector

14. *April 15, Reuters* – (National) **Right-wing group blamed in leak of U.S. officials' home addresses: CBS.** A spokesperson for DHS confirmed April 15 that the department had notified an unknown number of employees from various government agencies that had been identified in an online post that allegedly leaked a number of home addresses gathered from publicly available sources. The department encouraged the employees to be vigilant.
Source: http://www.reuters.com/article/2015/04/15/us-usa-security-addresses-idUSKBN0N61H120150415

15. *April 14, Corpus Christi Caller-Times* – (Texas) **Parts of Coastal Bend see lingering power outages, flooding.** An April 14 storm that moved across Texas prompted Crockett and Evans elementary schools, Martin Middle School, and Travis Elementary School to close due to power outages. Outages were also reported at Corpus Christi Gas Department, Broadmoor and Greenwood senior centers, and thousands of homes.
Source: http://www.caller.com/news/local-news/weather/severe-thunderstorm-flash-flood-warnings-in-effect

16. *April 14, WFXT 25 Boston* – (Massachusetts) **Southbridge students sent home after middle, high school evacuated.** Students at Southbridge Middle School/High School

in Massachusetts were evacuated and the school was closed April 14 while police investigated a suspicious package reportedly in the building. Authorities searched a student who had a device on him and cleared the scene after determining the device was a hoax.
Source: http://www.myfoxboston.com/story/28797717/southbridge-middle-school-and-high-school-evacuated

17. *April 14, Forum of Fargo-Moorhead* – (North Dakota; Minnesota) **Fires starting up almost daily across Minnesota and North Dakota.** The governor of North Dakota extended a Statewide fire emergency order April 14 through at least April 30 due to hot, dry, and windy weather conditions that have been igniting fires from western North Dakota to Minnesota. Classes were canceled at the University of Mary in Bismarck and students were evacuated when a grass fire threatened the university and nearby homes.
Source: http://www.inforum.com/news/3722787-fires-starting-almost-daily-across-minnesota-and-north-dakota

18. *April 14, U.S. Department of Justice* – (Maryland; Virginia) **Former DEA employee pleads guilty to credit card fraud scheme.** A former program manager for the Drug Enforcement Agency (DEA) pleaded guilty April 14 to defrauding the Federal government out of more than $113,000 by submitting at least 32 fraudulent credit card applications to JPMorgan Chase & Co., for fictitious DEA employees and using the cards to withdraw funds for personal use from ATMs in Maryland and Virginia.
Source: http://www.justice.gov/opa/pr/former-dea-employee-pleads-guilty-credit-card-fraud-scheme

For additional stories, see items **12**, **21**, and **26**

[Return to top]

Emergency Services Sector

19. *April 15, Scranton Times-Tribune* – (Pennsylvania) **Scranton fire station reopens after air test shows no mold problem.** East Mountain's fire station in Scranton reopened April 14 after closing April 9 as a precaution while investigators conducted air tests for mold after 2 firefighters complained of headaches. The air tests showed that there were no issues with mold.
Source: http://thetimes-tribune.com/news/scranton-fire-station-reopens-after-air-test-shows-no-mold-problem-1.1863487

20. *April 14, Associated Press* – (Delaware) **2 inmates caught, 1 at large after prison break in Delaware.** The Delaware Department of Corrections reported that 2 of 3 inmates were recaptured April 13 after all 3 prisoners scaled a wall to escape from the Plummer Community Corrections Center in Wilmington April 12. Authorities are still searching for the third inmate.
Source: http://6abc.com/news/2-inmates-caught-1-at-large-after-del-prison-break/658740/

[Return to top]

Information Technology Sector

21. *April 15, Softpedia* – (International) **Victim of cyber-attack replies with own backdoor.** Security researchers at Kaspersky Lab reported that it observed two cyberespionage advanced persistent threat (APT) groups called Hellsing and Naikon engage in deliberate APT-on-APT attacks through spear-phishing emails containing custom malware, signaling a potential new trend. Hellsing was previously linked to other APT groups and the group has targeted diplomatic organizations in the U.S.
Source: http://news.softpedia.com/news/Victim-of-Cyber-Attack-Replies-with-Own-Backdoor-478425.shtml

22. *April 15, Help Net Security* – (International) **Adobe fixes Flash Player zero-day exploited in the wild.** Adobe released a new version of Flash Player for Windows, Macintosh, and Linux that addresses 22 critical vulnerabilities, including one that is exploited in the wild and could lead to code execution and an attacker taking control of the affected system. A security bypass vulnerability that could lead to information disclosure and memory leak flaws that could be leveraged to bypass address space layout randomization (ALSR) also received fixes.
Source: http://www.net-security.org/secworld.php?id=18218

23. *April 15, Computerworld* – (International) **With latest patches, Oracle signals no more free updates for Java 7.** Oracle released patches addressing 14 vulnerabilities in Java as part of a 98 security-issue fix that covered multiple product lines and marked the end of free Java 7 updates. Three of the Java vulnerabilities were high severity and could be exploited over networks without authentication and could lead to a complete compromise of affected systems' confidentiality and integrity, and 12 others could be exploited from the Web through the Java browser plug-in.
Source: http://www.computerworld.com/article/2909908/with-latest-patches-oracle-signals-no-more-free-updates-for-java-7.html

24. *April 15, Securityweek* – (International) **Google fixes 45 security flaws with release of Chrome 42.** Google released Chrome 42 for Windows, Mac, and Linux, which included fixes for 45 security issues including a cross-origin bypass flaw in the HTML parser, a type confusion in V8, a use-after-free vulnerability in inter-process communication (IPC), and an out-of-bounds write bug in the Skia graphics engine, among others. The update also removed support for the Netscape Plugin Application Programming Interface (NPAPI).
Source: http://www.securityweek.com/google-fixes-45-security-flaws-release-chrome-42

25. *April 14, Network World* – (International) **Microsoft Patch Tuesday April 2015 closes 0-day holes: 4 of 11 patches rated critical.** Microsoft released 11 security bulletins that address 26 vulnerabilities, including critical remote code execution (RCE) flaws in Microsoft Office, a critical RCE vulnerability in HTTP.sys that could allow an attacker to use a malicious HTTP request to Windows Server to gain full remote control of a

system, and 9 critical security holes in Internet Explorer, among others.
Source: http://www.networkworld.com/article/2909627/microsoft-subnet/patch-tuesday-april-2015-closes-0-day-holes-4-of-11-patches-rated-critical-by-microsoft.html

26. *April 14, IDG News Service* – (International) **Web app attacks, PoS intrusions and cyberespionage leading causes of data breaches.** Findings from Verizon's recently released annual Data Breach Investigations Report revealed that the top industries affected by data breaches in the last year were public administration, financial services, manufacturing, accommodations, and retail, and that over two-thirds of cyberespionage incidents since 2013 involved phishing attacks. The report also determined that banking information and credentials were the most common records stolen, among other findings.
Source: http://www.networkworld.com/article/2909953/web-app-attacks-pos-intrusions-and-cyberespionage-leading-causes-of-data-breaches.html

27. *April 14, Threatpost* – (International) **Apple fixes cookie access vulnerability in safari on billions of devices.** A recent Apple update patched a cookie cross-domain vulnerability in all versions of the Safari Web browser on iOS, OS X, and Windows, that affected up to 1 billion devices, and was a result of the way Safari handled its file transfer protocol (FTP) uniform resource locator (URL) scheme, which could allow attackers to call upon documents to access and modify cookies belonging to Apple.com via JavaScript (JS). The update also patched a proxy manipulation vulnerability in iOS and multiple kernel vulnerabilities in OS X.
Source: https://threatpost.com/apple-fixes-cookie-access-vulnerability-in-safari-on-billions-of-devices/112246

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

28. *April 15, KSTP 5 St. Paul* – (Minnesota) **North Minneapolis fire burns in 4 buildings.** A 3-alarm fire that started inside a downtown Minneapolis commercial building April 15 caused the second floor to collapse before it spread to at least 3 additional structures and injured 1 person. The buildings were evacuated while

firefighters battled the blaze.
Source: http://kstp.com/article/stories/s3766462.shtml

29. *April 15, Los Angeles Daily News* – (California) **Suspicious package that caused evacuations near Beverly Center was environmental testing canister.** Several businesses and restaurants in Los Angeles were evacuated for about 3 hours April 14-15 while police investigated a suspicious package that was later determined to be an environmental testing canister.
Source: http://www.dailynews.com/general-news/20150415/suspicious-package-that-caused-evacuations-near-beverly-center-was-environmental-testing-canister

30. *April 15, Ardmore Main Line* – (Pennsylvania) **Police: 3 workers injured at King of Prussia Mall after cutting energized cable.** Three workers were injured April 13 at a construction site at the King of Prussia Mall in Upper Merion when a live cable was inadvertently severed by 2 of the individuals who were performing electrical work under the second floor from a scissor jack lift. Parts of the mall were without power for more than two hours, and officials inspected the site before it was declared safe and work resumed.
Source:
http://www.mainlinemedianews.com/articles/2015/04/15/king_of_prussia_courier/news/doc552cfeafbe570560561595.txt

31. *April 14, WPMT 43 York* – (Pennsylvania) **Military style truck slams into Subway store injuring four people.** A military style truck crashed into a Subway store in York County April 14 after the truck's brakes failed and caused the driver to lose control of the vehicle. Four patrons were transported to an area hospital with injuries.
Source: http://fox43.com/2015/04/14/military-style-truck-slams-into-subway-store-injuring-four-people/

32. *April 14, KCTV 5 Kansas City* – (Kansas) **Fire at Olathe business destroys strip mall.** Authorities continue to investigate the cause of a 3-alarm attic fire that damaged more than 4 stores at the Black Bob Corner Shopping Center in Olathe April 13. Patrons and staff were evacuated from the strip mall without incident.
Source: http://www.kctv5.com/story/28793239/attic-fire-reported-at-mexican-restaurant-in-olathe

For another story, see item **26**

[Return to top]

Dams Sector

Nothing to report

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer